UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,949	08/08/2006	David Arditti	33901-219PUS	2791

27799 7590 02/18/2009
COHEN, PONTANI, LIEBERMAN & PAVANE LLP
551 FIFTH AVENUE
SUITE 1210
NEW YORK, NY 10176

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
02/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/588,949	**Applicant(s)** ARDITTI ET AL.	
	Examiner MICHAEL R. VAUGHAN	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 August 2006* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/588,949 is presented for examination by the examiner. Claims

Response to Amendment

IDS

The IDS and its reference have been considered.

Drawings

The instantly filed amendment, claims to add new drawings sheets but they are not in the file. Please resubmit them.

Claim Objections

Claim objections have been overcome by the amendments.

Claim Rejections - 35 USC § 112

The instantly filed amendment has overcome the previous rejection and is thereby removed.

Response to Arguments

Applicant's arguments filed 12/22/08 have been fully considered but they are not persuasive. Applicant has alleged that the prior art of record fails to disclose all of the claim limitations but Examiner respectfully disagrees for the following reasons.

On page 16, of the response, Applicant alleges that Hind fails to teach claim 9's limitation of authenticating the device prior to delivering a certificate for a public key. Examiner's response to this allegation, is that this limitation is not in claim 9 so the point is moot.

Secondly, Applicant has alleged that Hind does not teach sending of a public certification key. Examiner does not see how one can interpret this term as being anything other than the public key which Hind sends to the administration server/CA in col. 10, lines 1-9. Clearly the device is making its public key known to the CA so that if some entity wishes to perform a secure message transaction with the device, the device can then send its public key, which has been certified by the CA, to the entity. The entity can then trust that the public key is from the device because it has been certified. It is well known that one uses the recipient's public key to encrypt messages intended to be sent to the recipient. The recipient then uses its private key to decrypt said messages.

Examiner appreciates the amendments made to the claims which solidify the original interpretation of the claim by removing 112 2nd paragraph problems. However, the amendments while requiring further consideration do not significantly narrow the limitations of the claims. As such, claim 9 is still rejected under 102 by Hind and claims

1-8 rejected by Hind in view of Farnham. Examiner has already stated that Hind does not explicitly teach the client device authenticating with the CA prior to certifying. As is well known in the art to do, Farnham teaches this process and it is obvious to modify Hind in such a way because Hind teaches of a secure communication between the device and CA. It only makes sense in a telecommunication network to only certify authentic devices (i.e. subscribers) in the network.

On page 19 of the response, Applicant alleges that Hinds fails to teach supplying the associated authenticated results to the CA. This falls under the authentication process taught by Farnham and therefore is also moot. Farnham sends an identifier as part of the authentication exchange to prevent a man-in-the-middle attack. This identifier would then convey the authentication result naturally, and only when the device is proven authentic will the CA accept the public key and certify it. This too is well known in the art of cryptographic communications.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim 9 is rejected under 35 U.S.C. 102(b) as being anticipated by USP 6,772,331 to Hind et al., hereinafter Hind.

As per claim 9, Hind teaches a mobile telecommunications terminal, comprising:

means for sending said key to a certification authority by means of a network call via a telephone network entity of the mobile telecommunications network such that said key produced by the mobile terminal becomes a public key which is used for encrypting messages received by the mobile terminal (col. 10, lines 5-10); and

means for storing the key produced by the mobile terminal (col. 10, lines 13-15).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind in view of USP Application Publication 2003/0210789 to Farnham et al., hereinafter Farnham.

As per claim 1, Hind teaches a certification method using a public key certification authority and involving at least one mobile terminal able to receive messages encrypted by that public key, wherein the method comprises:

the step of the mobile terminal generating the public key (col. 9, lines 65-67);

the step of a telecommunications network entity acquiring said key from the terminal by means of a network call (col. 10, lines 3-5); and

the step of supplying the certification authority with the public key and the associated result of the authentication process (col. 10, lines 5-10).

Hind teaches that the mobile terminal creates an encrypted session with the network entity. Hind also teaches various key agreements between devices which already have a certification (col. 10, lines 30-65). However, Hind does not explicitly teach that the mobile terminal authenticates itself to the network entity prior to the certification. Farnham teaches a process by which the network entity authenticates the terminal by a party authentication process used in relation to a standard telephone call (0014). Authentication is well known in the art and anyone of ordinary skill in computer security knows the importance of it. Combining the authentication method of Farnham which is very similar to the encryption method taught by Hind further strengthens the protocol. Farnham provides motivation for his authentication scheme as it eliminates a man-in-the-middle attack. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the authentication of the mobile terminal with the teaching of Hind to prevent an attacker from impersonating the mobile terminal.

As per claim 2, Hind does not explicitly teaches the authentication method of the mobile terminal includes the mobile terminal sending a calculation result involving a confidential key stored in the mobile terminal and the step of the network entity comparing the result with an expected result also calculated by the network entity using the same confidential key, a positive comparison result being interpreted as an identification of the mobile terminal. This authentication step is a Diffie Hellman key exchange. Hind does teach a Diffie Hellman key exchange as a way to form a session key (col. 10, lines 40-42). Farnham takes this a step further by using the public key of terminal as a means to authenticate the terminal to the server (0014). Examiner supplies the same rationale for combining Hind with Farnham as being obvious to one of ordinary skill in the art at the time of the invention.

As per claim 3, Hind does not explicitly teach the step of the network entity sending random data to the terminal and the step of the terminal calculating the random data sent by the network entity, the step of calculation by the network entity also involving said random data with a view to said comparison of results. Farnham teaches the step of the network entity sending random data to the terminal and the step of the terminal calculating the random data sent by the network entity, the step of calculation by the network entity also involving said random data with a view to said comparison of results (0014). Use of random data in an authentication protocol is both well known and taught by Farnham as a means to prevent replay attacks in securing a channel. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the random data in the authentication protocol to increase the difficulty in comprising the system.

As per claim 4, Hind teaches the step of the mobile terminal generating, in addition to the public key, a confidential key held in memory in the mobile terminal and used to decrypt received messages that were encrypted with the public key (col. 9, line 64).

As per claim 5, Hind teaches the terminal is adapted to send messages and to append to them an authentication signature produced using the confidential key that it previously generated itself (col. 11, lines 33-35).

As per claim 6, Hind teaches the step of the network entity sending the public key to the certification authority via a channel that is secured against unauthorized reading (col. 9, lines 37-39).

As per claim 7, Hind teaches the step of the mobile terminal using an authentication key of the mobile terminal usually employed in relation to telephone calls, generating an encryption key, encrypting messages using that encryption key and sending said messages (col. 10, lines 40-50).

As per claim 8, Hind teaches a mobile telecommunications system comprising:
at least one mobile terminal (col. 9, lines 66-67);
one network entity [administration server] (col. 10, lines 4-5);

means in the mobile terminal for generating a public key (col. 9, lines 66-67);
means in the telecommunications network entity for acquiring said public key from the mobile terminal by means of a network call (col. 10, lines 3-5);

a certification authority [CA] (col. 10, lines 9-10); and

means for supplying the certification authority with the public key generated by the mobile terminal and the associated result of the authentication process (col. 10, lines 9-10). Hind teaches that the mobile terminal creates an encrypted session with the network entity. Hind also teaches various key agreements between devices which already have a certification (col. 10, lines 30-65). However, Hind does not explicitly teach that the mobile terminal authenticates itself to the network entity prior to the certification. Farnham teaches a process by which the network entity authenticates the terminal by a party authentication process used in relation to a standard telephone call (0014). Authentication is well known in the art and anyone of ordinary skill in computer security knows the importance of it. Combining the authentication method of Farnham which is very similar to the encryption method taught by Hind further strengthens the protocol. Farnham provides motivation for his authentication scheme as it eliminates a man-in-the-middle attack. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the authentication of the mobile terminal with the teaching of Hind to prevent an attacker from impersonating the mobile terminal.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Syed Zia/

Primary Examiner, Art Unit 2431